IETF PQUIP
draft-ietf-pquip-pqc-engineers
“PQC For Engineers”

Tim Hollebeek

Aritra Banerjee, Tirumaleswar Reddy, Dimitrios Schoinianakis, Mike Ounsworth

2024-11-07

IETF 121 Dublin

PQC For Engineers

Quick recap of the draft

The draft explains why engineers need to be aware of and understand post-quantum cryptography.

It emphasizes the potential impact of Cryptographically Relevant Quantum Computers (CRQCs) on current cryptographic systems and the need to transition to post-quantum algorithms to ensure long-term security.

Adopted by the WG following IETF 117.

Since IETF 120

- Received lots and lots of useful comments.
- Major editorial pass by Paul Hoffman (THANK YOU!)
- No major changes.

Who is the Audience? (“What does the word engineer mean?”)

1. IETF protocol designers
2. Non-IETF developers who have to use PQC algorithms in new systems.
3. System maintainers who need to update their systems to be quantum-safe
4. Network operators who have to be able to install certs, manage smartcards, etc?
5. Crypto architects who have to manage HSMs?
6. Auditors who have to understand and evaluate cryptographic systems?

?

Current State of the Document

Comments from Yaakov Stein:

- "I think this document is really useful, but really really needs editorial work."

We agree. The authors really appreciate the extensive and thoughtful feedback we received. This is what we needed to move forward and will be spending lots of time on editorial work in the next few weeks.

Terms “PQC” and “Quantum Safe” A functional definition

- ML-DSA, ML-KEM, SLH-DSA and friends are “**Post-Quantum algorithms (PQC)**”. This is a class of technology.
- PQC algorithms can be used as building blocks within a “**Quantum Safe**” solution. This is a security property.
- Usage in a sentence:
  “My wizzpopper is quantum-safe because it uses PQC ciphersuites for TLS.”

- It was discussed extensively on the NIST pqc-list, and NIST decided to keep the term PQC.

“break”

- When we said “break”, we meant a pragmatic attack that significantly compromises the security properties (“Q-day”)
- Academic cryptographers use “break” in a different way. Reducing the strength of an algorithm is bad, even if it has no practical consequences. This is important, but different.

- We probably need a better word. The authors will revisit.

Algorithm names

COMMENT: “I realize that NIST uses ML-KEM but the original name "Kyber" is in such common use that it should be introduced.”

It’s not a choice, ML-KEM and Kyber are two different algorithms. One is interoperable and standardized, the other is not.

Thank you for your feedback!

The authors will incorporate the feedback and come back with an updated draft.